

Aiello 1999-0053

IN THE CLAIMS:

1. (Original) A method of provisioning a user's broadband telephony interface comprising the steps of:

receiving information authenticating a provisioning server;
establishing a communication channel between the user and the provisioning server over which is transmitted authorization information from the user to the provisioning server; and
encrypting and transmitting a cryptographic key associated with the user to the provisioning server.

2. (Currently Amended) The method of claim 34 1 further comprising the step of establishing a voice connection between said user and said network wherein the communication channel is a voice channel connection.

a1
3. (Currently Amended) The method of claim 2 further comprising said provisioning server sending a request to said user, over said voice connection, wherein the communication channel is encrypted using an audio channel with said complement of said key AK which is encrypted and transmitted to the provisioning server prior to establishing the communication channel.

4. (Currently Amended) The method of claim 2 3 wherein ~~the cryptographic key associated with the user is encrypted using a session key which is encrypted and transmitted to the provisioning server prior to establishing the communication channel~~ passes through said BTI.

5. (Currently Amended) The method of claim 4 wherein said key of said provisioning server is a public key the session key and the audio channel key are encrypted using a cryptographic key that is encrypted using a cryptographic key associated with the provisioning server and transmitted to the provisioning server with the encrypted session and audio channel key.

Aiello 1999-0053

6. (Currently Amended) The method of claim 5 wherein said acknowledgement is encrypted with said complement of said key SK ~~the cryptographic key associated with the provisioning server is received with the information authenticating the provisioning server.~~

7. (Currently Amended) The method of claim 6 wherein a random nonce is included in said tuple ~~with the encrypted session key.~~

8. (Currently Amended) The method of claim 34 + wherein the information that authenticates ~~authenticating~~ the provisioning server is a digital certificate.

a
9. (Currently Amended) The method of claim 34 + wherein any number of said keys taken from the set consisting of K, AK, and SK are symmetric keys, where a symmetric key is equal to its complement ~~the cryptographic key associated with the user is a symmetric key.~~

10. (Currently Amended) The method of claim 34 + wherein ~~the cryptographic key associated with the user~~ said complement of said key K is a public key and said key K is corresponding to a private key stored in the broadband telephony interface.

11. (Original) The method of claim 34 + wherein a hash is included with each transmission.

12. (Currently Amended) Apparatus broadband telephony interface comprising:

a first interface to a landline user telephone;

a second interface to a communication network with access to a provisioning server;

memory for storing cryptographic keys;

Aiello 1999-0053

a processor connected to the memory and the first and second interfaces for executing program instructions, the program instructions causing the processor to perform the steps of:

receiving a key of said provisioning server and information authenticating the provisioning server;

generating a random key K and its complement, a random session key SK and its complement, and a random audio channel key AK and its complement, where a complement of a key J is a key that decrypts messages message encrypted with said key J; establishing a communication channel between the user telephone and the provisioning server over which is transmitted authorization information from the user to the provisioning server; and

sending to said provisioning server information that includes said complement of said K encrypted with said key of said provisioning server, and a tuple encrypted with said K, which tuple includes said complement of said SK, and said complement of said AK encrypting and transmitting a cryptographic key associated with the user to the provisioning server.

13. (Currently Amended) The apparatus broadband telephony interface of claim 12 wherein the processor also generates a public/private key pair, and sends the public key to said provisioning server, communication channel is a voice channel connection.

14. (Currently Amended) The apparatus broadband telephony interface of claim ~~13~~ 12 wherein the communication channel is encrypted using an audio channel key which is encrypted and transmitted to the provisioning server prior to establishing the processor establishes a session communication channel with said provisioning server.

15. (Currently Amended) The apparatus broadband telephony interface of claim 14 wherein the processor communicates with said provisioning server over said session cryptographic key associated with the user is encrypted using a session key which is encrypted and transmitted to the provisioning server prior to establishing the

Aiello 1999-0053

communication channel by sending messages encrypted with said key SK, and receiving messages encrypted with said complement of said key SK.

16. (Canceled).

17. (Canceled).

18. (Currently Amended) The apparatus broadband telephony interface of claim 17 wherein a random nonce is included in said tuple with the encrypted session key.

21
19. (Currently Amended) The apparatus broadband telephony interface of claim 12 wherein the information authenticating the provisioning server is a digital certificate.

20. (Currently Amended) The apparatus broadband telephony interface of claim 12 wherein the cryptographic key K associated with the user is a symmetric key.

21. (Canceled).

22. (Original) The broadband telephony interface of claim 12 wherein a hash is included with each transmission.

23. (Canceled).

24. (Canceled).

25. (Canceled).

26. (Canceled).

Aiello 1999-0053

27. (Canceled).

28. (Canceled).

29. (Canceled).

30. (Canceled).

31. (Canceled).

32. (Canceled).

33. (Canceled).

34. (New) A method of employing a user's broadband telephony interface (BTI), executed in said BTI in communication with a network, comprising the steps of:

sending a request to a provisioning server;

receiving a key of said provisioning server and information that authenticates said provisioning server;

generating a random key K and its complement, a random session key SK and its complement, and a random audio channel key AK and its complement, where a complement of a key J is a key that decrypts messages message encrypted with said key J;

sending to said provisioning server information that includes said complement of said K encrypted with said key of said provisioning server, and a tuple encrypted with said K, which tuple includes said complement of said SK, and said complement of said AK; and

receiving an acknowledgement from said provisioning server.

35. (New) The method of claim 3 further comprising the steps of:

relaying said request to said user;

Aiello 1999-0053

receiving responsive information from said user; and
forwarding said responsive information to said provisioning server, encrypted
with said key AK.

36. (New) The method of claim 35 further comprising the steps of:
generating a public/private key pair; and
sending the generated public key to said provisioning server, encrypted with said
key SK.

37. (New) The method of claim 36 further comprising the step of receiving an
acknowledgement message from said provisioning server, in response to said sending of
the generated public key, which acknowledgement message is encrypted with said
complement of said key SK.

38. (New) The method of claim 34 + wherein said step of sending to said
provisioning server includes information encrypted with said key SK.

39. (New) The method of claim 38 wherein said information encrypted with said
key SK provides an address of said BTL.